

0300
GEGGROE ÁI ÁFIGJÁÚT
SÖÖÁUWVY
ÚWÚÖÜÜÁÁUWÜVÁÖŠÖÜS
ÖÖÖÖ
ÖÖÜÖÁKÖGÖÖ I HĚ ÁÜÖÖ

**SUPERIOR COURT OF WASHINGTON
IN AND FOR KING COUNTY**

JEFFRIE ALAN SUMMERS II, on behalf of
himself and all others similarly situated,

Plaintiff,

vs.

SEA MAR COMMUNITY HEALTH CENTERS,

Defendant.

No.

CLASS ACTION COMPLAINT

JURY DEMAND

TABLE OF CONTENTS

		<u>Page</u>
1		
2		
3	I. INTRODUCTION	3
4	II. PARTIES	9
5	III. JURISDICTION AND VENUE	9
6	IV. FACTUAL ALLEGATIONS	9
7	A. Background	9
8	B. Defendant's Privacy Policy	10
9	C. The Data Breach	11
10	D. Defendant's Failures Before and After the Data Breach	16
11	E. The Healthcare Sector is Particularly Susceptible to Data Breaches	18
12	F. Defendant Acquires, Collects and Stores Plaintiff and Class Members' PII and PHI.	20
13	G. Securing PII and Preventing Breaches	20
14	H. Value of Personal Identifiable Information	21
15	I. Defendant's Conduct Violates HIPAA	24
16	J. Defendant Failed to Comply with FTC Guidelines	26
17	K. Plaintiff and Class Members Suffered Damages	28
18	L. Plaintiff Jeffrie Alan Summers II's Experience	28
19	V. CLASS ALLEGATIONS	29
20	COUNT I NEGLIGENCE (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)	32
21	COUNT II BREACH OF EXPRESS CONTRACT (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)	38
22	COUNT III BREACH OF IMPLIED CONTRACT (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)	40
23	COUNT IV INVASION OF PRIVACY (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)	43
24	COUNT V BREACH OF CONFIDENCE (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)	44
25		
26		
27		
28		

COUNT VI VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT, WASH. REV. CODE § 19.86.020, <i>ET SEQ.</i> (ON BEHALF OF PLAINTIFF AND THE WASHINGTON SUBCLASS).....	47
COUNT VII VIOLATION OF THE WASHINGTON DATA BREACH STATUTE WASH. REV. CODE § 19.255.010(1), <i>ET. SEQ.</i> (ON BEHALF OF PLAINTIFF AND THE WASHINGTON SUBCLASS).....	49
COUNT VIII WASHINGTON UNIFORM HEALTH CARE INFORMATION ACT, WASH. REV. CODE §§ 70.02.020, <i>ET SEQ.</i> ; § 70.02.170, <i>ET SEQ.</i> (ON BEHALF OF PLAINTIFF AND THE WASHINGTON SUBCLASS).....	50
PRAYER FOR RELIEF	51
DEMAND FOR JURY TRIAL	53

1 Plaintiff Jeffrie Alan Summers II (“Plaintiff”), individually and on behalf of all others
 2 similarly situated (“Class Members”), brings this Class Action Complaint against Sea Mar
 3 Community Health Centers (“Sea Mar” or “Defendant”), and alleges, upon personal knowledge as
 4 to his own actions and his counsels’ investigations, and upon information and belief as to all other
 5 matters, as follows:

6 I. INTRODUCTION

7 1. Plaintiff brings this class action against Defendant for its failure to properly secure
 8 and safeguard personally identifiable information and protected health information (“PHI”) that
 9 Defendant’s patients entrusted to it. This information included, without limitation, name, address,
 10 Social Security number, date of birth, client identification number, diagnostic and treatment
 11 information, insurance information, claims information, and/or images associated with dental
 12 treatment (collectively, “personally identifiable information” or “PII”).¹ Defendant failed to
 13 comply with industry standards to protect information systems that contained Class Members
 14 PII and PHI, and failed to provide timely, accurate, and adequate notice to Plaintiff and other Class
 15 Members that their PII and PHI had been accessed and copied by an unauthorized third
 16 party. Plaintiff also alleges that Defendant failed to provide timely, accurate, and adequate notice
 17 to Plaintiff and Class Members of precisely what types of information was unencrypted and in the
 18 possession of unknown third parties. Plaintiff seeks, among other things, orders requiring
 19 Defendant to fully and accurately disclose the nature of the information that has been
 20 compromised, to adopt reasonably sufficient security practices and safeguards to prevent incidents
 21 like the disclosure in the future, to destroy information no longer necessary to retain for the
 22 purposes that the information was first obtained from Class Members, and to provide a sum of
 23 money sufficient to provide to Plaintiff and Class Members identity theft protective services for
 24
 25

26 ¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace
 27 an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. §
 28 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is
 generally defined to include certain identifiers that do not on their face name an individual, but that are considered to
 be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number,
 driver’s license number, financial account number).

1 their respective lifetimes as Plaintiff and Class Members will be at an increased risk of identity
2 theft due to the conduct of Sea Mar described herein.

3 2. Sea Mar Community Health Centers is a private non-profit health care system with
4 over 90 facilities across Washington.² In 2020, Sea Mar served over 304,000 patients and
5 employed over 2,700 individuals.³ According to public records, Sea Mar's total assets at the end
6 of 2020 exceeded \$280 million and net assets exceeded \$145 million.⁴

7 3. Plaintiff and Class Members, as patients of Defendant and Defendant's affiliated
8 health care providers, entrusted Defendant with an extensive amount of their PII and
9 PHI. Defendant retained this information on its "digital environment"—even after the relationship
10 ended.

11 4. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class
12 Members' PII and PHI, Defendant assumed legal and equitable duties to Plaintiff and Class
13 Members. Defendant asserts that it understands the importance of protecting such information.

14 5. Defendant's "Notice Privacy Practices" ("Privacy Policy") is posted on its website.
15 The Privacy Policy states: "Sea Mar Community Health Centers respects your privacy. We
16 understand that your personal health information is very sensitive. We will not disclose your
17 information to others unless you tell us to do so, or unless the law authorizes or requires us to do
18 so."⁵

19 6. The Privacy Policy states that Defendant collects, among other things, personal
20 health information, including "symptoms, test results, diagnoses, treatment, health information
21 from other providers, and billing and payment information relating to these services."⁶

24 ² See <http://www.seamar.org/> (last visited Nov. 22, 2021).

25 ³ SEA MAR, 2020 *Annual Report*, at 8-10, available at <https://www.seamar.org/seamar-downloads/Annual-Report2020.pdf> (last visited Nov. 22, 2021).

26 ⁴ See https://projects.propublica.org/nonprofits/display_990/911020139/04_2021_prefixes_87-91%2F911020139_202003_990_2021041217926132 (last visited Nov. 22, 2021).

27 ⁵ Ex. 1 (Notice of Privacy Practices), available at <https://www.seamar.org/notice.html> (last visited Nov. 22, 2021).

28 ⁶ *Id.*

7. Further, under “Other Uses and Disclosures of Protected Health Information,” the Privacy Policy states “[u]ses and disclosures not in this Notice will be made only as allowed or required by law or with your written authorization.”⁷

8. In addition, Defendant’s website contains a form contract entitled “Notice of Privacy Practices Acknowledgement” (“Privacy Acknowledgement”) with a signature line underneath the words “I acknowledge receipt of Sea Mar Community Health Centers’ Notice of Privacy Practices and Patient Rights and Responsibilities.”⁸

9. On or about June 24, 2021, Defendant “was informed that certain Sea Mar data had been copied from its digital environment by an unauthorized actor.” Upon investigation, Defendant learned that “additional data may have been removed from its digital environment between December 2020 and March 2021” (the “Data Breach”).⁹

10. At the time of the Data Breach, the PII and PHI of Plaintiff and Class Members were accessible from the internet, despite any security mechanisms that Defendant wrongly believed would safeguard the PII and PHI from unauthorized access.

11. At the time of the Data Breach, none of the PII and PHI was encrypted.

12. At the time of the Data Breach, the PII and PHI included information that Defendant no longer had a reasonable need to maintain.

13. Despite admitting that it learned of the Data Breach as early as June 24, 2021, Defendant claims the process of collecting the contact information required to issue notification letters to affected individuals was completed on August 30, 2021.

14. On or about October 29, 2021, at least *four months after* it learned of the Data Breach, Defendant posted a *Notice of Data Security Incident* on its website.¹⁰ Only on or about that date did Defendant begin notifying Plaintiff and Class Members of the Data Breach.

⁷ *Id.*

⁸ Ex. 2 (Notice of Privacy Practices Acknowledgement), available at https://www.seamar.org/seamar-downloads/covid/PatientAcknow_ENG.pdf (last visited Nov. 22, 2021).

⁹ See Ex. 3 (Defendant’s *Notice of Data Security Incident*), available at https://www.seamar.org/seamar-downloads/2021-10-28-Breach_Notice.pdf.

¹⁰ Ex. 3 (Defendant’s *Notice of Data Security Incident*), available at https://www.seamar.org/seamar-downloads/2021-10-28-Breach_Notice.pdf.

1 15. On or about October 30, 2021, Defendant reported to the Department of Health and
2 Human Services that the Data Breach compromised the unprotected health information of *more*
3 *than 688,000* current or former Sea Mar patients.¹¹

4 16. On or about November 5, 2021, Defendant began notifying various states Attorneys
5 General of the Data Breach.¹²

6 17. For example, on or about November 5, 2021, Defendant notified the Maine
7 Attorney General of the breach.¹³ According to the Maine Attorney General's website, Defendant
8 reported that the breach occurred and/or began on December 12, 2020 and was discovered on
9 August 30, 2021. Defendant reported to the Maine Attorney General that the breach affected a
10 total of 651,500 individuals.

11 18. Defendant, in its *Notice of Data Incident* and its sample Breach Notification Letters,
12 stated that it was not aware of any evidence of the misuse of information stolen in the incident.¹⁴
13 However, news reports indicate this information Defendant allowed to be compromised already
14 has found its way to the Dark Web, where it may be bought, sold and transferred in perpetuity,
15 causing victims of the Data Breach untold harm. As early as June of 2021, information from the
16 Data Breach was offered for sale on Marketo, a Dark Web data leak website. On October 30, 2021,
17 *DataBreaches.net* reported:

18 [o]n some exact date that is unknown to DataBreaches.net, threat actors
19 gained access to Sea Mar's network and exfiltrated what they claimed was
20 3 TB of data. The incident was posted on Marketo's leaked data site in June.
21 **In Sea Mar's case, Marketo claimed to have 201 bids for their data back**
22 **in July.**¹⁵

23 ¹¹ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=1F20E164939520967E5581395A557BCD
24 (last visited Nov. 22, 2021).

25 ¹² See Ex. 4 (sample *Notice of Data Breach* filed with Maine Attorney General); Ex. 5 (sample *Notice of Data Breach* filed with California Attorney General).

26 ¹³ <https://apps.web.maine.gov/online/aeviewer/ME/40/7a7933d5-1c49-44ec-99ec-fbdc873ae915.shtml> (last
27 visited Nov. 22, 2021).

28 ¹⁴ Ex. 1.

¹⁵ DATABREACHES.COM, *Sea Mar Community Health Centers Discloses Breach That Began Last Year*,
<https://www.databreaches.net/wa-sea-mar-community-health-centers-discloses-breach-that-began-last-year/> (last
visited Nov. 22, 2021) (emphasis added).

1 19. According to reporting, Sea Mar did not respond to *four separate inquiries* about
2 the attack and the listing on Marketo that were sent to Defendant beginning June 24, 2021.¹⁶ The
3 four inquiries were sent through Defendant's website as well as through Twitter Direct Message.¹⁷

4 20. Despite these inquiries about the attack and the Marketo listing, Defendant did not
5 disclose the Data Breach to Plaintiff, Class Members, or the relevant state and federal authorities
6 until more than four months had passed since Defendant was first informed of the Data Breach.
7 Additionally, as of filing, Defendant has not yet disclosed the misappropriation and/or potential
8 sale of affected individuals' information to Plaintiff and Class Members.

9 21. Defendant's delays virtually ensured that the individuals who exploited
10 Defendant's security failure(s) could monetize, misuse, and/or disseminate Plaintiff and Class
11 Members' PII and PHI before Plaintiff and Class Members could take affirmative steps to protect
12 their identities.

13 22. The exposed PII and PHI of Plaintiff and Class Members was placed into the hands
14 of criminals. Since at least last December, hackers and cybercriminals have had access to the
15 unencrypted, unredacted PII and PHI of more than 688,000 individuals, and since at least June of
16 2021, that PII and PHI has been available for purchase on the Dark Web.

17 23. Plaintiff and Class Members face a lifetime risk of identity theft, which is
18 heightened here by the loss of Social Security numbers. Plaintiff and Class Members are currently
19 suffering and for the rest of their lifetimes will suffer the significant and concrete risk that their
20 identities will be (or already have been) misused—a virtual certainty given that Plaintiff's and
21 Class Members' PII and/or PHI were being sold on the Dark Web long before Defendant notified
22 Plaintiff and Class Members of the Data Breach.

23 24. This PII and PHI was compromised, exfiltrated, and offered for sale on the Dark
24 Web due to Defendant's negligent and/or careless acts and omissions and the failure to protect the
25 PII and PHI of Plaintiff and Class Members.

26
27 ¹⁶ *Id.*

28 ¹⁷ *See id.*

1 25. Plaintiff brings this action on behalf of all persons whose PII and PHI was accessed,
2 acquired, and/or misappropriated as a result of Defendant's failure to: (i) adequately protect the
3 PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its
4 inadequate information security practices; and (iii) avoid sharing the PII and PHI of Plaintiff and
5 Class Members without adequate safeguards. Defendant's conduct amounts to negligence and
6 violates federal and state statutes.

7 26. Additionally, as a result of Defendant's failure to follow contractually-agreed upon,
8 federally-prescribed, industry standard security procedures, Plaintiff and Class Members received
9 only a diminished value of the services Defendant had agreed to provide.

10 27. Plaintiff and Class Members have suffered injuries as a result of Defendant's
11 conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket
12 expenses associated with the prevention, detection, and recovery from identity theft, tax fraud,
13 and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting
14 to mitigate the actual consequences of the Data Breach, including, but not limited to, lost time, and
15 significantly (iv) the ongoing and increased risk to their PII and PHI, which: (a) remains
16 unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain
17 backed up in Defendant's possession and is subject to further unauthorized disclosures so long as
18 Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI it
19 maintains on its systems.

20 28. Defendant disregarded the rights of Plaintiff and Class Members by intentionally,
21 willfully, recklessly, or negligently failing to take and implement adequate and reasonable
22 measures to ensure that Plaintiff's and Class Members' PII and PHI was safeguarded, failing to
23 take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,
24 required and appropriate protocols, policies and procedures regarding the encryption of data, even
25 for internal use.

26 29. As a result, the PII and PHI of Plaintiff and Class Members was accessed,
27 exfiltrated, and/or sold by an unknown and unauthorized third party. Plaintiff and Class Members
28

1 have a continuing interest in ensuring that their information is and remains safe, and they should
2 be entitled to injunctive and other equitable relief.

3 **II. PARTIES**

4 30. Plaintiff Jeffrie Alan Summers II is a citizen of Washington, residing in Lacey,
5 Washington.

6 31. Defendant Sea Mar Community Health Centers is a Washington corporation with
7 its principal place of business in Seattle, Washington. Defendant is headquartered at 1040 S.
8 Henderson Street, Seattle, WA 98108.

9 32. The true names and capacities of persons or entities, whether individual, corporate,
10 associate, or otherwise, who may be responsible for some of the claims alleged herein are currently
11 unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true
12 names and capacities of such other responsible parties when their identities become known.

13 33. All of Plaintiff's claims stated herein are asserted against Defendant and any of its
14 owners, predecessors, successors, subsidiaries, agents and/or assigns.

15 **III. JURISDICTION AND VENUE**

16 34. This Court has jurisdiction and venue pursuant to Wash. Rev. Code § 4.12.020 and
17 Wash. Rev. Code § 4.12.025 because Defendant resides in King County and on information and
18 belief the acts and failures to act that caused Plaintiff's damages occurred in King County.

19 **IV. FACTUAL ALLEGATIONS**

20 **A. Background**

21 35. As a condition of providing medical care, Defendant collected and stored Plaintiff's
22 and Class Members' most sensitive and confidential person and medical information, including,
23 without limitation, name, address, Social Security number, date of birth, client identification
24 number, diagnostic and treatment information for medical, vision, dental, and orthodontic care,
25 medical, vision, and dental insurance information, claims information, and/or images associated
26 with dental treatment. This includes information that is static, does not change, and can be used to
27 commit myriad financial crimes.
28

36. Plaintiff and Class Members relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII and PHI.

37. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII and PHI from involuntary disclosure to third parties.

B. Defendant's Privacy Policy

38. Defendant's "Notice of Privacy Practices" ("Privacy Policy"), located under Patients/Clients on its website, describes "how medical information about you may be used and disclosed, and how you can get access to this information." The Privacy Policy asks for patients and clients to "[p]lease review it carefully."¹⁸

39. The Privacy Policy states: "Sea Mar Community Health Centers respects your privacy. We understand that your personal health information is very sensitive. We will not disclose your information to others unless you tell us to do so, or unless the law authorizes or requires us to do so."¹⁹

40. The Privacy Policy states that Defendant collects, among other things, personal health information, including "symptoms, test results, diagnoses, treatment, health information from other providers, and billing and payment information relating to these services."²⁰

41. The Privacy Policy also states:

The law protects the privacy of the health information we create and obtain in providing health care and services to you. [. . .] Federal and state law allows us to use and disclose your protected health information for purposes of treatment and health care operations to others. State law requires us to get your authorization to disclose this information for payment purposes.²¹

¹⁸ Ex. 1 (Notice of Privacy Practices) (emphasis added), available at <https://www.seamar.org/notice.html> (last visited Nov. 22, 2021).

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

Under “Other Uses and Disclosures of Protected Health Information,” the Privacy Policy states “[u]ses and disclosures not in this Notice will be made only as allowed or required by law or with your written authorization.”²²

42. Under “Our Responsibilities” the Privacy Policy states:

We are required to:

- Keep your protected health information private;
- Give you this Notice;
- Follow the terms of this Notice.

We have the right to change our practices regarding the protected health information we maintain. If we make changes, we will update this Notice.²³

43. In addition, Defendant’s website contains a form contract entitled “Notice of Privacy Practices Acknowledgement” (“Privacy Acknowledgement”) with a signature line underneath the words “I acknowledge receipt of Sea Mar Community Health Centers’ Notice of Privacy Practices and Patient Rights and Responsibilities.”²⁴

44. The Privacy Acknowledgment states, in part:

Sea Mar has the responsibility to protect the privacy of your information, provide a Notice of Privacy Practices, and follow information practices that are described in this notice. [. . .] By signing this form, you acknowledge receipt of Sea Mar Community Health Centers’ Notice of Privacy Practices and Patient Rights and Responsibilities. Sea Mar encourages you to review these notices carefully.²⁵

C. The Data Breach

45. On or about October 29, 2021, Defendant posted a *Notice of Data Security Incident* on its website.²⁶ It read, in part, as follows:

Sea Mar Community Health Centers (“Sea Mar”), a non-profit organization that provides healthcare services to underserved communities in the state of Washington, has learned of a data

²² *Id.*

²³ *Id.*

²⁴ Ex. 2 (*Notice of Privacy Practices Acknowledgement*), available at https://www.seamar.org/seamar-downloads/covid/PatientAcknow_ENG.pdf (last visited Nov. 22, 2021).

²⁵ *Id.*

²⁶ Ex. 3 (*Defendant’s Notice of Data Security Incident*), available at https://www.seamar.org/seamar-downloads/2021-10-28-Breach_Notice.pdf (last visited Nov. 22, 2021).

1 security incident that may have involved personal and protected
2 health information belonging to certain current and former Sea Mar
3 patients. Sea Mar has sent notification of this incident to potentially
4 impacted individuals and has provided resources to assist them.

5 On June 24, 2021, Sea Mar was informed that certain Sea Mar data
6 had been copied from its digital environment by an unauthorized
7 actor. Upon receipt of this information, Sea Mar immediately took
8 steps to secure its environment and commenced an investigation to
9 determine what happened and to identify the specific information
10 that may have been impacted. In so doing, Sea Mar engaged leading,
11 independent cybersecurity experts for assistance. As a result, Sea
12 Mar learned that additional data may have been removed from its
13 digital environment between December 2020 and March 2021. Sea
14 Mar thereafter began collecting contact information needed to
15 provide notice to potentially affected individuals, which was
16 completed on August 30, 2021.

17 Sea Mar is not aware of any evidence of the misuse of any
18 information potentially involved in this incident. However,
19 beginning on October 29, 2021, Sea Mar provided of this incident
20 to the potentially impacted individuals. In so doing, Sea Mar
21 provided information about the incident and about steps that
22 potentially impacted individuals can take to protect their
23 information. Sea Mar takes the security and privacy of patient
24 information very seriously and is taking steps to prevent a similar
25 event from occurring in the future.

26 The following personal and protected health information may have
27 been involved in the incident: Name, address, Social Security
28 number, date of birth, client identification number, medical / vision
/ dental / orthodontic diagnostic and treatment information, medical
/ vision / dental insurance information, claims information, and / or
images associated with dental treatment. [. . .]

The privacy and protection of personal and protected health
information is a top priority for Sea Mar, which deeply regrets any
inconvenience or concern this incident may cause.

***While we are not aware of the misuse of any potentially affected
individual's information, we are providing the following
information to help those wanting to know more about steps they
can take to protect themselves and their personal information.²⁷***

²⁷ Ex. 3 (emphasis in original).

1 46. On or about October 29, 2021, Defendant began notifying Plaintiff and Class
2 Members of the Data Breach.

3 47. On or about October 30, 2021, Defendant reported to the Department of Health and
4 Human Services that, during the Data Breach, the attacker compromised the unprotected health
5 information of more than 688,000 current or former patients of Defendant.²⁸

6 48. On or about November 5, 2021, Defendant began notifying various states Attorneys
7 General of the Data Breach. On or about November 5, 2021, Defendant informed the Maine,
8 California, Massachusetts, and Montana Attorneys General of the Data Breach.²⁹ The fact of these
9 notifications indicates that Defendant's records show that PII from persons in each of these states
10 was affected. On November 15, 2021, Defendant informed the Washington State Attorney General
11 of the Data Breach.³⁰

12 49. For example, on or about November 5, 2021, Defendant notified the Maine
13 Attorney General of the breach.³¹ Defendant reported to the Maine Attorney General that the
14 breach affected a total of 651,500 individuals. Defendant included a sample Data Breach
15 Notification Letter, substantially similar to the California sample letter and the form *Notice of a*
16 *Data Breach* sent to Plaintiff and Class Members. Defendant, through counsel, also included a
17 letter to Maine Attorney General Frey, which stated that "[o]n June 24, 2021, Defendant was
18 informed that certain Sea Mar data had been **removed** from the Sea Mar digital environment."³²

19 50. On or about October 29, 2021, Defendant sent Plaintiff and Class Members a form
20 *Notice of Data Breach*, substantially similar to the California and Maine sample letters.³³
21 Defendant informed Plaintiff and Class Members as follows:

22
23 ²⁸ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=1F20E164939520967E5581395A557BCD
(last visited Nov. 22, 2021).

24 ²⁹ See Ex. 4 (sample *Notice of Data Breach* filed with Maine Attorney General); Ex. 5 (sample *Notice of Data*
25 *Breach* filed with California Attorney General); Ex. 6 (sample *Notice of Data Breach* filed with Massachusetts
Attorney General); Ex. 7 (sample *Notice of Data Breach* filed with Montana Attorney General).

26 ³⁰ See Ex. 8 (sample *Notice of Data Breach* filed with Washington Attorney General), available at
<https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachM11218.pdf> (last visited Jan. 10, 2022).

27 ³¹ <https://apps.web.maine.gov/online/aeviewer/ME/40/7a7933d5-1c49-44ec-99ee-fbdc873ae915.shtml> (last
visited Nov. 22, 2021).

28 ³² Ex. 4 (emphasis added).

³³ See Ex. 4; Ex. 5.

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers (“Sea Mar”) that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident and steps that you can take to help protect your information.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, Social Security number, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

What We Are Doing: As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.³⁴

³⁴ See Ex. 4; Ex. 5.

1 51. On October 30, 2021 and November 5, 2021, Defendant notified various state
 2 Attorneys General of the Data Breach. Defendant also provided the Attorneys General with letters
 3 and/or “sample” notices of the Data Breach that reaffirm the compromised information included
 4 “name, address, Social Security number, date of birth, client identification number,
 5 medical/vision/dental/orthodontic diagnostic and treatment information, medical/vision/dental
 6 insurance information, claims information, and/or images associated with dental treatment.”³⁵

7 52. Defendant admitted in the sample breach notices that an unauthorized party
 8 compromised sensitive information about Plaintiff and Class Members, including, name, address,
 9 Social Security number, date of birth, client identification number,
 10 medical/vision/dental/orthodontic diagnostic and treatment information, medical/vision/dental
 11 insurance information, claims information, and/or images associated with dental treatment.

12 53. In response to the Data Breach, Defendant claims that it is “working with
 13 cybersecurity experts to identify areas in which it can further improve the security of its network
 14 to reduce the likelihood of a similar event occurring in the future”³⁶ However, the details of the
 15 root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken
 16 to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class
 17 Members, who retain a vested interest in ensuring that their information remains protected.

18 54. News reports indicate some or all of Plaintiff and Class Members PII and PHI that
 19 Defendant allowed to be compromised already has found its way to the Dark Web, where it may
 20 be bought, sold and transferred in perpetuity, causing victims of the Data Breach untold harm.
 21 Alternatively, the wrongfully accessed, acquired, and/or misappropriated PII and PHI could simply
 22 fall into the hands of companies that will use the detailed PII and/or PHI for targeted marketing
 23 without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access
 24 the PII and PHI of Plaintiff and Class Members.

25
 26
 27
 28 ³⁵ Ex. 4.

³⁶ Ex. 4.

55. Defendant did not use reasonable security procedures and practices appropriate to the nature of Plaintiff's and Class Members' sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII and PHI to be exposed.

D. Defendant's Failures Before and After the Data Breach

56. As early as June of 2021, information from the Data Breach was offered for sale on a Dark Web data leak website, Marketo. According to HIPAA JOURNAL, Marketo is a "darknet marketplace where stolen data are offered for sale."³⁷

57. On October 30, 2021, *DataBreaches.net* reported:

[o]n some exact date that is unknown to DataBreaches.net, threat actors gained access to Sea Mar's network and exfiltrated what they claimed was 3 TB of data. The incident was posted on Marketo's leaked data site in June. In Sea Mar's case, *Marketo claimed to have 201 bids for their data back in July*.³⁸

58. According to the article, "Marketo uploaded a small proof of claims archive of files," as is customary for listings on the site, DataBreaches.net says. "It contained a few photos of identified pediatric dental patients. Each one held a sign with their name, date of birth, and date of photo."³⁹ A photo of the listing on Marketo is included below.

³⁷ HIPAA JOURNAL, *PHI of 688,000 Individuals Compromised in Sea Mar Community Health Centers Hack* (Nov. 16, 2021), available at <https://www.hipaajournal.com/phi-of-1-27-million-patients-compromised-in-two-healthcare-data-breaches/> (last visited Nov. 22, 2021).

³⁸ DATABREACHES.COM, *Sea Mar Community Health Centers Discloses Breach That Began Last Year*, <https://www.databreaches.net/wa-sea-mar-community-health-centers-discloses-breach-that-began-last-year/> (last visited Nov. 22, 2021).

³⁹ *Id.*



59. According to the article, Sea Mar did not respond to inquiries sent to it on June 24, 2021, about the attack and listing on Marketo. The article further states that Sea Mar did not respond “to requests sent to it via its web site on [July 21, 2021] and via Twitter DM on [July 21, 2021] or a fourth request sent on [July 28, 2021].”⁴⁰

60. The listing on Marketo is no longer available as of November 24, 2021, however a cached web archive from November 10, 2021 indicates the listing was live at least until that date.⁴¹ The heading for the listing, as of that date, had changed to “**Starting publication of Critical Data.**” The listing stated as follows.

Sea Mar Community Health Centers is a community-based organization committed to providing health, human, housing, educational and cultural services to diverse communities, specializing in service to Latinos in Washington state. Your attempts at tolerance do not make up for other sins. You serve all persons without regard to race, ethnicity, immigration status, gender, or sexual orientation, and regardless of ability to pay for services. But you decided to forget without remorse about the quality of the

⁴⁰ *Id.*

⁴¹ GOOGLE WEBCACHE, *Cache of Marketo Listing from November 10, 2021* <https://webcache.googleusercontent.com/search?q=cache:KQZ6B165qd8J:https://marketo.cloud/lot/51/+&cd=1&hl=en&ct=clnk&gl=us> (last visited Nov. 24, 2021).

provided services and the clients' right to confidentiality. Customers do not come to you for services so that photos of their sick, crooked teeth are publicly available. Their beautiful, contended smiles are just a part of the interesting data leaked online. Personal letters (emails), photos and contacts of clients, photos of agreements - here is a worthy reason to smile for your customers, partners and competitors, because your accent on tolerance led to poor-quality services and allowed hacking. Say "cheese" and smile with your beautiful teeth.⁴²

61. Defendant, in its sample Breach Notification Letters, stated numerous times that it was not aware of misuse of information stolen in the incident or any evidence thereof. According to an article dated November 16, 2021, from HIPAA JOURNAL:

No mention is made in the breach notification letters about the stolen data being listed for sale on Marketo. [. . .]

The date of notification provided by Sea Mar corresponds with the date DataBreaches.net notified Sea Mar of the listing on Marketo.⁴³

E. The Healthcare Sector is Particularly Susceptible to Data Breaches

62. Defendant was on notice that companies in the healthcare industry are targets for data breaches.

63. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."⁴⁴

64. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

⁴² *Id.*

⁴³ HIPAA JOURNAL, *PHI of 688,000 Individuals Compromised in Sea Mar Community Health Centers Hack* (Nov. 16, 2021), available at <https://www.hipaajournal.com/phi-of-1-27-million-patients-compromised-in-two-healthcare-data-breaches/> (last visited Nov. 22, 2021).

⁴⁴ Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), available at: <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820> (last visited Sept. 27, 2020).

Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.⁴⁵

65. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a 40 percent increase in the number of data breaches from the previous year.⁴⁶ In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.⁴⁷ That trend continues.

66. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.⁴⁸ Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about \$20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.⁴⁹ Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.⁵⁰

67. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security

⁴⁵ Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), available at: <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals> (last visited Sept. 27, 2020).

⁴⁶ Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), available at: <https://www.idtheftcenter.org/surveys-studys> (last visited Sept. 27, 2020).

⁴⁷ Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, available at: <https://www.idtheftcenter.org/2017-data-breaches/> (last visited Sept. 18, 2020).

⁴⁸ Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, available at: <https://www.idtheftcenter.org/2018-data-breaches/> (last visited Sept. 18, 2020).

⁴⁹ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), available at: <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last visited Sept. 28, 2020).

⁵⁰ *Id.*

1 incident in the last 12 months, with a majority of these known incidents being caused by “bad
 2 actors” such as cybercriminals.⁵¹ “Hospitals have emerged as a primary target because they sit on
 3 a gold mine of sensitive personally identifiable information for thousands of patients at any given
 4 time. From social security and insurance policies, to next of kin and credit cards, no other
 5 organization, including credit bureaus, have so much monetizable information stored in their data
 6 centers.”⁵²

7 **F. Defendant Acquires, Collects and Stores Plaintiff and Class Members’ PII and PHI.**

8 68. Defendant acquired, collected, and stored Plaintiff and Class Members’ PII and
 9 PHI.

10 69. As a condition of its relationships with Plaintiff and Class Members, Defendant
 11 required that Plaintiff and Class Members entrust Defendant with this highly confidential PII and
 12 PHI.

13 70. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class
 14 Members, Defendant assumed legal and equitable duties and knew or should have known that it
 15 was responsible for protecting the PII and PHI from disclosure.

16 71. Plaintiff and Class Members have taken reasonable steps to maintain the
 17 confidentiality of their PII and PHI and relied on Defendant to keep their PII and PHI confidential
 18 and securely maintained, to use this information for business purposes only, and to make only
 19 authorized disclosures of this information.

20 **G. Securing PII and Preventing Breaches**

21 72. Defendant could have prevented this Data Breach by properly securing and
 22 encrypting the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have
 23 destroyed data it no longer needed, especially years-old data from former patients.

26 ⁵¹ 2019 HIMSS Cybersecurity Survey, available at: <https://www.himss.org/2019-himss-cybersecurity-survey>
 27 (last visited Sept. 28, 2020).

28 ⁵² Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available
 at: <https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last visited
 Sept. 28, 2020).

73. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

74. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

75. Despite allegedly receiving four separate inquiries regarding the attack and the listing on Marketo, Defendant failed to take appropriate steps to warn and notify Plaintiff and Class Members of the Data Breach and the Dark Web data dump.

76. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."⁵³ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."⁵⁴

77. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

H. Value of Personal Identifiable Information

78. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite dark-web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.⁵⁵ Experian reports that a stolen credit or debit

⁵³ 17 C.F.R. § 248.201 (2013).

⁵⁴ *Id.*

⁵⁵ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Apr. 5, 2021).

card number can sell for \$5 to \$110 on the Dark Web.⁵⁶ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.⁵⁷

79. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.⁵⁸

80. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

81. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."⁵⁹

⁵⁶ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Apr. 5, 2021).

⁵⁷ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Apr. 5, 2021).

⁵⁸ SOCIAL SECURITY ADMINISTRATION, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed Apr. 5, 2021).

⁵⁹ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last accessed Apr. 5, 2021).

82. Further, there is a market for Plaintiff's and Class Members PHI, and the stolen PII and PHI has inherent value. Sensitive healthcare data can sell for as much as \$363 per record according to the Infosec Institute.⁶⁰

83. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

84. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."⁶¹

85. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

Cyber criminals are selling [medical] information on the black market at a rate of \$50 for each partial EHR, compared to \$1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.⁶²

⁶⁰ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), available at: <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last accessed June 6, 2021).

⁶¹ Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News (Feb. 7, 2014) available at: <https://khn.org/news/rise-of-identity-theft/> (last accessed June 6, 2021).

⁶² FBI Cyber Division, Private Industry Notification, "(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," Apr. 8, 2014, available at: <http://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf> (last visited June 6, 2021).

86. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—name, Social Security number, medical records, and potentially date of birth.

87. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”⁶³

88. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

89. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

90. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁶⁴

I. Defendant’s Conduct Violates HIPAA

91. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the

⁶³ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Apr. 5, 2021).

⁶⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/products/gao-07-737> (last accessed Apr. 5, 2021).

1 Department of Health and Human Services (“HHS”) create rules to streamline the standards for
 2 handling PII like the data Defendant left unguarded. The HHS has subsequently promulgated five
 3 rules under authority of the Administrative Simplification provisions of HIPAA.

4 92. Defendant’s Data Breach resulted from a combination of insufficiencies that
 5 indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry
 6 standards. First, it can be inferred from Defendant’s Data Breach that Defendant either failed to
 7 implement, or inadequately implemented, information security policies or procedures in place to
 8 protect Plaintiff and Class Members’ PII and PHI.

9 93. In addition, Defendant’s Data Breach could have been prevented if Defendant
 10 implemented HIPAA mandated, industry standard policies and procedures for securely disposing
 11 of PII and PHI when it was no longer necessary and/or had honored its obligations to its patients.

12 94. Defendant’s security failures also include, but are not limited to:

- 13 a. Failing to maintain an adequate data security system to prevent data loss;
- 14 b. Failing to mitigate the risks of a data breach and loss of data;
- 15 c. Failing to ensure the confidentiality and integrity of electronic protected
 16 health information Defendant creates, receives, maintains, and transmits in
 violation of 45 C.F.R. § 164.306(a)(1);
- 17 d. Failing to implement technical policies and procedures for electronic
 18 information systems that maintain electronic protected health information
 to allow access only to those persons or software programs that have been
 19 granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- 20 e. Failing to implement policies and procedures to prevent, detect, contain,
 21 and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- 22 f. Failing to identify and respond to suspected or known security incidents;
 23 mitigate, to the extent practicable, harmful effects of security incidents that
 are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- 24 g. Failing to protect against any reasonably-anticipated threats or hazards to
 25 the security or integrity of electronic protected health information in
 violation of 45 C.F.R. § 164.306(a)(2);
- 26 h. Failing to protect against any reasonably-anticipated uses or disclosures of
 27 electronic protected health information that are not permitted under the
 28 privacy rules regarding individually identifiable health information in
 violation of 45 CFR 164.306(a)(3);

- i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(94);
- j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*; and
- k. Retaining information past a recognized purpose and not deleting it.

95. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and *in no case later than 60 days following discovery of the breach.*"⁶⁵

96. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiff and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the protected health information and other PII of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff and Class Members' protected health information and other PII remains at risk of subsequent Data Breaches.

J. Defendant Failed to Comply with FTC Guidelines

97. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

98. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁶⁶

⁶⁵ Breach Notification Rule, U.S. DEP'T OF HEALTH & HUMAN SERVICES, *available at*: hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Oct. 13, 2020).

⁶⁶ FEDERAL TRADE COMMISSION, *Start With Security: A Guide for Business*, *available at*: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed Sept. 27, 2020).

1 99. In 2016, the FTC updated its publication, *Protecting Personal Information: A*
 2 *Guide for Business*, which established cybersecurity guidelines for businesses.⁶⁷ The guidelines
 3 note that businesses should protect the personal customer information that they keep; properly
 4 dispose of personal information that is no longer needed; encrypt information stored on computer
 5 networks; understand their network's vulnerabilities; and implement policies to correct any
 6 security problems.

7 100. The FTC further recommends that companies not maintain PII longer than is
 8 needed for authorization of a transaction; limit access to private data; require complex passwords
 9 to be used on networks; use industry-tested methods for security; monitor for suspicious activity
 10 on the network; and verify that third-party service providers have implemented reasonable security
 11 measures.⁶⁸

12 101. The FTC has brought enforcement actions against businesses for failing to
 13 adequately and reasonably protect customer data, treating the failure to employ reasonable and
 14 appropriate measures to protect against unauthorized access to confidential consumer data as an
 15 unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting
 16 from these actions further clarify the measures businesses must take to meet their data security
 17 obligations.

18 102. Defendant failed to properly implement basic data security practices. Defendant's
 19 failure to employ reasonable and appropriate measures to protect against unauthorized access to
 20 patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the
 21 FTC Act, 15 U.S.C. § 45.

22 103. Defendant was at all times fully aware of its obligation to protect the PII of patients
 23 because of its position as a leading healthcare provider. Defendant was also aware of the significant
 24 repercussions that would result from its failure to do so.

25
 26
 27 ⁶⁷ FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business*, available at:
https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last
 28 accessed Sept. 27, 2020).

⁶⁸ FTC, *Start With Security*, *supra*.

K. Plaintiff and Class Members Suffered Damages

104. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result.

105. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

106. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system, amounting to more than 656,000 individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

107. To date, Defendant has offered Plaintiff and Class Members whose Social Security numbers were released only one year of identity monitoring services through a single provider, Kroll. Enrollment in the service is only available until January 27, 2021. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

108. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

L. Plaintiff Jeffrie Alan Summers II's Experience

109. Two and a half years ago, Plaintiff sought dental care at one of Defendant's facilities. As a condition of that care, Plaintiff was required to provide his personal and medical information, including his Social Security number.

110. Plaintiff last visited one of Defendant's facilities approximately one year ago.

111. On or about October 29, 2021, Plaintiff received a Notice of Data Breach from Defendant.

1 112. As a result of the Data Breach, Plaintiff spent time dealing with the consequences
2 of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited
3 emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft
4 insurance options, attempting to enroll in the credit monitoring and identity theft protection
5 services offered by Defendant, and self-monitoring his accounts. This time has been lost forever
6 and cannot be recaptured.

7 113. Additionally, Plaintiff is very careful about sharing his PII. He has never knowingly
8 transmitted unencrypted PII over the internet or any other unsecured source.

9 114. Plaintiff stores any documents containing his PII in a safe and secure location.
10 Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

11 115. Plaintiff suffered actual injury in the form of damages to and diminution in the
12 value of his PII—a form of intangible property that Plaintiff entrusted to Defendant for the purpose
13 of obtaining healthcare from Defendant, which was compromised in and as a result of the Data
14 Breach.

15 116. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result
16 of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

17 117. Plaintiff has suffered injury arising from the present and continuing risk of fraud,
18 identity theft, and misuse resulting from his PII and PHI, especially his Social Security number, in
19 combination with his name, being placed in the hands of unauthorized third parties and possibly
20 criminals.

21 118. Plaintiff has a continuing interest in ensuring that his PII, which, upon information
22 and belief, remain backed up in Defendant's possession, is protected and safeguarded from future
23 breaches.

24 V. CLASS ALLEGATIONS

25 119. Plaintiff brings this nationwide class action on behalf of himself and on behalf of
26 all others similarly situated pursuant to Wash. Sup. Cr. Civ. R. 23, and other applicable law.

27 120. The Nationwide Class that Plaintiff seeks to represent is defined as follows:
28

All individuals residing in the United States whose PII and/or PHI was accessed, acquired, and/or removed during the data breach referenced in the *Notice of Data Security Incident* Sea Mar Community Health Centers posted on October 29, 2021 (the “Nationwide Class”).

121. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a separate subclass, defined as follows:

All individuals residing in Washington whose PII and/or PHI was accessed, acquired, and/or removed during the data breach referenced in the *Notice of Data Security Incident* Sea Mar Community Health Centers posted on October 29, 2021 (the “Washington Subclass”).

122. Excluded from the Class and subclass are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff members.

123. Plaintiff reserves the right to modify or amend the definition of the proposed Class and subclass before the Court determines whether certification is appropriate.

124. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class-wide relief because Plaintiff and all members of the Nationwide Class were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

125. The Nationwide Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are at least hundreds of thousands of Class Members. Defendant advised the Department of Health and Human Services that the breach affected at least 688,000 individuals.

126. Common questions of law and fact exist as to members of the Nationwide Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

- a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;
- b. Whether Defendant had a duty not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had a duty not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

127. Plaintiff is a member of the Class and alternative subclass he seeks to represent and his claims and injuries are typical of the claims and injuries of the other Class and subclass members.

1 information, medical/vision/dental insurance information, claims information, and/or images
2 associated with dental treatment.

3 133. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendant on the
4 premise and with the understanding that Defendant would safeguard their information, use their
5 PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third
6 parties.

7 134. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of
8 harm that Plaintiff and the Nationwide Class could and would suffer if the PII and PHI were
9 wrongfully disclosed.

10 135. Defendant knew or reasonably should have known that the failure to exercise due
11 care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Nationwide Class
12 involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm
13 occurred through the criminal acts of a third party.

14 136. Defendant had a duty to exercise reasonable care in safeguarding, securing, and
15 protecting such information from being compromised, lost, stolen, misused, and/or disclosed to
16 unauthorized parties. This duty includes, among other things, designing, maintaining, and testing
17 Defendant's security protocols to ensure that the PII and PHI of Plaintiff and the Nationwide Class
18 in Defendant's possession was adequately secured and protected.

19 137. Defendant also had a duty to exercise appropriate clearinghouse practices to remove
20 PII and PHI it was no longer required to retain pursuant to regulations, including that of former
21 customers or patients.

22 138. Defendant also had a duty to have procedures in place to detect and prevent the
23 improper access and misuse of the PII and PHI of Plaintiff and the Nationwide Class.

24 139. Defendant's duty to use reasonable security measures arose as a result of the special
25 relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special
26 relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their
27 confidential PII and PHI, a necessary part of their relationships with Defendant.

1 140. Defendant was subject to an “independent duty,” untethered to any contract
2 between Defendant and Plaintiff or the Nationwide Class.

3 141. A breach of security, unauthorized access, and resulting injury to Plaintiff and the
4 Nationwide Class was reasonably foreseeable, particularly in light of Defendant’s inadequate
5 security practices.

6 142. Plaintiff and the Nationwide Class were the foreseeable and probable victims of
7 any inadequate security practices and procedures. Defendant knew or should have known of the
8 inherent risks in collecting and storing the PII and PHI of Plaintiff and the Nationwide Class, the
9 critical importance of providing adequate security of that PII and PHI, and the necessity for
10 encrypting PII and PHI stored on Defendant’s systems.

11 143. Defendant’s own conduct created a foreseeable risk of harm to Plaintiff and the
12 Nationwide Class. Defendant’s misconduct included, but was not limited to, its failure to take the
13 steps and opportunities to prevent the Data Breach as set forth herein. Defendant’s misconduct
14 also included its decisions not to comply with industry standards for the safekeeping of the PII and
15 PHI of Plaintiff and the Nationwide Class, including basic encryption techniques freely available
16 to Defendant.

17 144. Plaintiff and the Nationwide Class had no ability to protect their PII and PHI that
18 was in, and possibly remains in, Defendant’s possession.

19 145. Defendant was in a position to protect against the harm suffered by Plaintiff and
20 the Nationwide Class as a result of the Data Breach.

21 146. Defendant had and continues to have a duty to adequately disclose that the PII and
22 PHI of Plaintiff and the Nationwide Class within Defendant’s possession might have been
23 compromised, how it was compromised, and precisely the types of data that were compromised
24 and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to
25 prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third
26 parties.

27 147. Defendant had a duty to employ proper procedures to prevent the unauthorized
28 dissemination of the PII and PHI of Plaintiff and the Nationwide Class.

1 148. Defendant has admitted that the PII and PHI of Plaintiff and the Nationwide Class
2 was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

3 149. Defendant, through its actions and/or omissions, unlawfully breached its duties to
4 Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise
5 reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide
6 Class during the time the PII and PHI was within Defendant's possession or control.

7 150. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiff
8 and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the
9 time of the Data Breach.

10 151. Defendant failed to heed industry warnings and alerts to provide adequate
11 safeguards to protect the PII and PHI of Plaintiff and the Nationwide Class in the face of increased
12 risk of theft.

13 152. Defendant, through its actions and/or omissions, unlawfully breached its duty to
14 Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and
15 prevent dissemination of their PII and PHI.

16 153. Defendant breached its duty to exercise appropriate clearinghouse practices by
17 failing to remove PII and PHI it was no longer required to retain pursuant to regulations.

18 154. Defendant, through its actions and/or omissions, unlawfully breached its duty to
19 adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of
20 the Data Breach.

21 155. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and
22 the Nationwide Class, the PII and PHI of Plaintiff and the Nationwide Class would not have been
23 compromised.

24 156. There is a close causal connection between Defendant's failure to implement
25 security measures to protect the PII and PHI of Plaintiff and the Nationwide Class and the harm,
26 or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII and PHI of
27 Plaintiff and the Nationwide Class was compromised as the proximate result of Defendant's failure
28

1 to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and
2 maintaining appropriate security measures.

3 157. Additionally, Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting
4 commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by
5 businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The
6 FTC publications and orders described above also form part of the basis of Defendant’s duty in
7 this regard.

8 158. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures
9 to protect PII and PHI and not complying with applicable industry standards, as described in detail
10 herein. Defendant’s conduct was particularly unreasonable given the nature and amount of PII and
11 PHI it obtained and stored and the foreseeable consequences of the immense damages that would
12 result to Plaintiff and the Nationwide Class.

13 159. Defendant’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

14 160. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act
15 was intended to protect.

16 161. The harm that occurred as a result of the Data Breach is the type of harm the FTC
17 Act was intended to guard against. The FTC has pursued enforcement actions against businesses,
18 which, as a result of their failure to employ reasonable data security measures and avoid unfair and
19 deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

20 162. Defendant’s violation of HIPAA also independently constitutes negligence *per se*.

21 163. HIPAA privacy laws were enacted with the objective of protecting the
22 confidentiality of patients’ healthcare information and set forth the conditions under which such
23 information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to
24 healthcare providers and the organizations they work for, but to any entity that may have access to
25 healthcare information about a patient that—if it were to fall into the wrong hands—could present
26 a risk of harm to the patient’s finances or reputation.

27 164. Plaintiff and the Nationwide Class are within the class of persons that HIPAA
28 privacy laws were intended to protect.

1 165. The harm that occurred as a result of the Data Breach is the type of harm HIPAA
2 privacy laws were intended to guard against.

3 166. As a direct and proximate result of Defendant's negligence and negligence *per se*,
4 Plaintiff and the Nationwide Class have suffered and will suffer injury, including, but not limited
5 to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the
6 compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated
7 with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use
8 of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of
9 productivity addressing and attempting to mitigate the actual and future consequences of the Data
10 Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and
11 recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit
12 reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and
13 are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate
14 and adequate measures to protect the PII and PHI of Plaintiff and the Nationwide Class; and (viii)
15 future costs in terms of time, effort, and money that will be expended to prevent, detect, contest,
16 and repair the impact of the PII and PHI compromised as a result of the Data Breach for the
17 remainder of the lives of Plaintiff and the Nationwide Class.

18 167. As a direct and proximate result of Defendant's negligence and negligence *per se*,
19 Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury
20 and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other
21 economic and non-economic losses.

22 168. Additionally, as a direct and proximate result of Defendant's negligence and
23 negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer the continued
24 risks of exposure of their PII and PHI, which remain in Defendant's possession and are subject to
25 further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
26 measures to protect the PII and PHI in its continued possession.

**BREACH OF EXPRESS CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

171. Defendant required Plaintiff and the Nationwide Class to provide and entrust to it their PII and PHI, including, without limitation, name, address, Social Security number, date of birth, client identification number, medical/vision/dental/orthodontic diagnostic and treatment information, medical/vision/dental insurance information, claims information, and/or images associated with dental treatment as a condition of obtaining medical care from Defendant.

173. Further, under “Other Uses and Disclosures of Protected Health Information,” the Privacy Policy states “[u]ses and disclosures not in this Notice will be made only as allowed or required by law or with your written authorization.”⁷⁰ Defendant provided a list of instances in which disclosure could be made absent written permission, none of which is at issue here.

174. In addition, Defendant’s website contains a form contract entitled “Notice of Privacy Practices Acknowledgement” (“Privacy Acknowledgement”) with a signature line underneath the words “I acknowledge receipt of Sea Mar Community Health Centers’ Notice of Privacy Practices and Patient Rights and Responsibilities.”⁷¹

⁷¹ Ex. 2.

1 175. A meeting of the minds occurred when Plaintiff and the Nationwide Class agreed
2 to, and did, provide their PII and PHI to Defendant, in exchange for, amongst other things, the
3 protection of their PII and PHI.

4 176. As a condition of obtaining care from Defendant, Plaintiff and the Nationwide Class
5 provided and entrusted their personal information. In so doing, Plaintiff the Nationwide Class
6 entered into contracts with Defendant by which Defendant agreed to safeguard and protect such
7 information, to keep such information secure and confidential, and to timely and accurately notify
8 Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

9 177. Plaintiff and the Nationwide Class fully performed their obligations under the
10 contracts with Defendant.

11 178. Defendant breached the contracts it made with Plaintiff and the Nationwide Class
12 by failing to safeguard and protect their personal and financial information and by failing to
13 provide timely and accurate notice to them that personal and financial information was
14 compromised as a result of the data breach.

15 179. As a direct and proximate result of Defendant's above-described breach of contract,
16 Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent,
17 and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and
18 economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and
19 economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the
20 compromised data on the Dark Web; expenses and/or time spent on credit monitoring and identity
21 theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports;
22 expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work
23 time; and other economic and non-economic harm.

24 180. As a result of Defendant's breach of contract, Plaintiff and the Nationwide Class
25 are entitled to and demand actual, consequential, and nominal damages.
26
27
28

COUNT III

**BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

181. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 130.

182. Defendant required Plaintiff and the Nationwide Class to provide and entrust to it their PII and PHI, including, without limitation, name, address, Social Security number, date of birth, client identification number, medical/vision/dental/orthodontic diagnostic and treatment information, medical/vision/dental insurance information, claims information, and/or images associated with dental treatment as a condition of obtaining medical care from Defendant.

183. As described above, Defendant's Privacy Policy Defendant's ("Privacy Policy") is posted on its website. Privacy Policy states: "Sea Mar Community Health Centers respects your privacy. We understand that your personal health information is very sensitive. We will not disclose your information to others unless you tell us to do so, or unless the law authorizes or requires us to do so."⁷²

184. Further, under "Other Uses and Disclosures of Protected Health Information," the Privacy Policy states "[u]ses and disclosures not in this Notice will be made only as allowed or required by law or with your written authorization."⁷³ Defendant provided a list of instances in which disclosure could be made absent written permission, none of which is at issue here.

185. In addition, Defendant's website contains a form contract entitled "Notice of Privacy Practices Acknowledgement" ("Privacy Acknowledgement") with a signature line underneath the words "I acknowledge receipt of Sea Mar Community Health Centers' Notice of Privacy Practices and Patient Rights and Responsibilities."⁷⁴

⁷² Ex. 1.

⁷³ *Id.*

⁷⁴ Ex. 2.

1 186. Defendant solicited and invited Plaintiff and the Nationwide Class to provide their
2 PII and PHI as part of Defendant's regular business practices. Plaintiff and the Nationwide Class
3 accepted Defendant's offers and provided their PII and PHI to Defendant.

4 187. As a condition of obtaining care from Defendant, Plaintiff and the Nationwide Class
5 provided and entrusted their personal information. In so doing, Plaintiff the Nationwide Class
6 entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect
7 such information, to keep such information secure and confidential, and to timely and accurately
8 notify Plaintiff and the Nationwide Class if their data had been breached and compromised or
9 stolen.

10 188. A meeting of the minds occurred when Plaintiff and the Nationwide Class agreed
11 to, and did, provide their PII and PHI to Defendant, in exchange for, amongst other things, the
12 protection of their PII and PHI.

13 189. Plaintiff and the Nationwide Class fully performed their obligations under the
14 implied contracts with Defendant.

15 190. Defendant further breached the implied contracts with Plaintiff and the Nationwide
16 Class by failing to comply with its promise to abide by HIPAA.

17 191. Defendant further breached the implied contracts with Plaintiff and the Nationwide
18 Class by failing to ensure the confidentiality and integrity of electronic protected health
19 information Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. §
20 164.306(a)(1).

21 192. Defendant further breached the implied contracts with Plaintiff and the Nationwide
22 Class by failing to implement technical policies and procedures for electronic information systems
23 that maintain electronic protected health information to allow access only to those persons or
24 software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

25 193. Defendant further breached the implied contracts with Plaintiff and the Nationwide
26 Class by failing to implement policies and procedures to prevent, detect, contain, and correct
27 security violations in violation of 45 C.F.R. § 164.308(a)(1).
28

1 194. Defendant further breached the implied contracts with Plaintiff and the Nationwide
2 Class by failing to identify and respond to suspected or known security incidents; mitigate, to the
3 extent practicable, harmful effects of security incidents that are known to the covered entity in
4 violation of 45 C.F.R. § 164.308(a)(6)(ii).

5 195. Defendant further breached the implied contracts with Plaintiff and the Nationwide
6 Class by failing to protect against any reasonably anticipated threats or hazards to the security or
7 integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2).

8 196. Defendant further breached the implied contracts with Plaintiff and the Nationwide
9 Class by failing to protect against any reasonably anticipated uses or disclosures of electronic
10 protected health information that are not permitted under the privacy rules regarding individually
11 identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

12 197. Defendant further breached the implied contracts with Plaintiff and the Nationwide
13 Class by failing to ensure compliance with the HIPAA security standard rules by its workforce
14 violations in violation of 45 C.F.R. § 164.306(a)(94).

15 198. Defendant further breached the implied contracts with Plaintiff and the Nationwide
16 Class by impermissibly and improperly using and disclosing protected health information that is
17 and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*

18 199. Defendant further breached the implied contracts with Plaintiff and the Nationwide
19 Class by failing to design, implement, and enforce policies and procedures establishing physical
20 administrative safeguards to reasonably safeguard protected health information, in compliance
21 with 45 C.F.R. § 164.530(c).

22 200. Defendant breached the implied contracts it made with Plaintiff and the Nationwide
23 Class by failing to safeguard and protect their personal and financial information and by failing to
24 provide timely and accurate notice to them that personal and financial information was
25 compromised as a result of the data breach.

26 201. As a direct and proximate result of Defendant's above-described breach of implied
27 contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing,
28 imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary

1 loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss
2 and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of
3 the compromised data on the Dark Web; expenses and/or time spent on credit monitoring and
4 identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit
5 reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost
6 work time; and other economic and non-economic harm.

7 202. As a result of Defendant's breach of implied contract, Plaintiff and the Nationwide
8 Class are entitled to and demand actual, consequential, and nominal damages.

9 **COUNT IV**

10 **INVASION OF PRIVACY**
11 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

12 203. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all
13 of the allegations contained in paragraphs 1 through 130.

14 204. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their
15 PII and PHI and were entitled to the protection of this information against disclosure to
16 unauthorized third parties.

17 205. Defendant owed a duty to its current and former patients, including Plaintiff and
18 the Nationwide Class, to keep their PII and PHI contained as a part thereof, confidential.

19 206. Defendant failed to protect and released to unknown and unauthorized third parties
20 the PII and PHI of Plaintiff and the Nationwide Class.

21 207. Defendant allowed unauthorized and unknown third parties to access and examine
22 of the PII and PHI of Plaintiff and the Nationwide Class, by way of Defendant's failure to protect
23 the PII and PHI.

24 208. The unauthorized release to, custody of, and examination by unauthorized third
25 parties of the PII and PHI of Plaintiff and the Nationwide Class is highly offensive to a reasonable
26 person.

27 209. The intrusion was into a place or thing, which was private and is entitled to be
28 private. Plaintiff and the Nationwide Class disclosed their PII and PHI to Defendant as part of

1 Plaintiff's and the Nationwide Class's relationships with Defendant, but privately with an intention
 2 that the PII and PHI would be kept confidential and would be protected from unauthorized
 3 disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information
 4 would be kept private and would not be disclosed without their authorization.

5 210. The Data Breach at the hands of Defendant constitutes an intentional interference
 6 with Plaintiff's and the Nationwide Class's interest in solitude or seclusion, either as to their
 7 persons or as to their private affairs or concerns, of a kind that would be highly offensive to a
 8 reasonable person.

9 211. Defendant acted with a knowing state of mind when it permitted the Data Breach
 10 to occur because it was with actual knowledge that its information security practices were
 11 inadequate and insufficient.

12 212. Because Defendant acted with this knowing state of mind, it had notice and knew
 13 the inadequate and insufficient information security practices would cause injury and harm to
 14 Plaintiff and the Nationwide Class.

15 213. As a proximate result of the above acts and omissions of Defendant, the PII and
 16 PHI of Plaintiff and the Nationwide Class was disclosed to third parties without authorization,
 17 causing Plaintiff and the Nationwide Class to suffer damages.

18 214. Unless and until enjoined, and restrained by order of this Court, Defendant's
 19 wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the
 20 Nationwide Class in that the PII and PHI maintained by Defendant can be viewed, distributed, and
 21 used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no
 22 adequate remedy at law for the injuries in that a judgment for monetary damages will not end the
 23 invasion of privacy for Plaintiff and the Nationwide Class.

24 **COUNT V**

25 **BREACH OF CONFIDENCE** 26 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

27 215. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all
 28 of the allegations contained in paragraphs 1 through 130.

1 216. At all times during Plaintiff's and the Nationwide Class's interactions with
2 Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and
3 the Nationwide Class's PII and PHI that Plaintiff and the Nationwide Class provided to Defendant.

4 217. As alleged herein and above, Defendant's relationship with Plaintiff and the
5 Nationwide Class was governed by terms and expectations that Plaintiff's and the Nationwide
6 Class's PII and PHI would be collected, stored, and protected in confidence, and would not be
7 disclosed to unauthorized third parties.

8 218. Plaintiff and the Nationwide Class provided their PII and PHI to Defendant with
9 the explicit and implicit understandings that Defendant would protect and not permit the PII and
10 PHI to be disseminated to any unauthorized third parties.

11 219. Plaintiff and the Nationwide Class also provided their PII and PHI to Defendant
12 with the explicit and implicit understandings that Defendant would take precautions to protect that
13 PII and PHI from unauthorized disclosure.

14 220. Defendant voluntarily received in confidence the PII and PHI of Plaintiff and the
15 Nationwide Class with the understanding that PII and PHI would not be disclosed or disseminated
16 to the public or any unauthorized third parties.

17 221. Due to Defendant's failure to prevent and avoid the Data Breach from occurring,
18 the PII and PHI of Plaintiff and the Nationwide Class was disclosed and misappropriated to
19 unauthorized third parties beyond Plaintiff's and the Nationwide Class's confidence, and without
20 their express permission.

21 222. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff
22 and the Nationwide Class have suffered damages.

23 223. But for Defendant's disclosure of Plaintiff's and the Nationwide Class's PII and
24 PHI in violation of the parties' understanding of confidence, their PII and PHI would not have
25 been compromised by unauthorized third parties. The Data Breach was the direct and legal cause
26 of the theft of Plaintiff's and the Nationwide Class's PII and PHI as well as the resulting damages.

27 224. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably
28 foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Nationwide Class's

1 PII and PHI. Defendant knew or should have known its methods of accepting and securing
2 Plaintiff's and the Nationwide Class's PII and PHI was inadequate as it relates to, at the very least,
3 securing servers and other equipment containing Plaintiff's and the Nationwide Class's PII and
4 PHI.

5 225. As a direct and proximate result of Defendant's breach of its confidence with
6 Plaintiff and the Nationwide Class, Plaintiff and the Nationwide Class have suffered and will suffer
7 injury, including, but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how
8 their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv)
9 out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft,
10 tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with
11 effort expended and the loss of productivity addressing and attempting to mitigate the actual and
12 future consequences of the Data Breach, including but not limited to efforts spent researching how
13 to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with
14 placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in
15 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant
16 fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and
17 the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be
18 expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a
19 result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

20 226. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff
21 and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or
22 harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic
23 and non-economic losses.

24 227. As a result of Defendant's breaches of confidence, Plaintiff and the Nationwide
25 Class are entitled to and demand actual, consequential, and nominal damages.
26
27
28

COUNT VI

**VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT,
WASH. REV. CODE § 19.86.020, *ET SEQ.*
(ON BEHALF OF PLAINTIFF AND THE WASHINGTON SUBCLASS)**

228. Plaintiff and the Washington Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 130.

229. Washington’s Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq.* (“CPA”), protects both consumers and competitors by promoting fair competition in commercial markets for goods and services. To achieve that goal, the CPA prohibits any person from using “unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce[.]” Wash. Rev. Code § 19.86.020.

230. As alleged herein, Defendant’s policies and practices relating to its substandard security measures for the use and retention of its patients’ personal and medical information violate the CPA because they are both unfair and deceptive. Further, Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of the CPA, including, but not limited to, the following:

- a. Defendant misrepresented and fraudulently advertised material facts pertaining to the health care services to the Washington Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Washington Subclass Members’ PII and PHI from unauthorized disclosure, release, data breaches, and theft;
- b. Defendant misrepresented material facts pertaining to health care services to the Washington Subclass by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Washington Subclass Members’ PII and PHI;
- c. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Washington Subclass Members’ PII and PHI;
- d. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff and Washington Subclass Members’ PII and PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by

laws including Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq.*), and the Washington regulations pertaining to Privacy of Health Care Information (Wash. Rev. Code §§ 70.02.020, *et seq.*; § 70.02.170, *et seq.*).

- e. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiff and the Washington Subclass in a timely and accurate manner, contrary to the duties imposed by § 19.255.010(1);
- f. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to have appropriate security safeguards or controls in place to prevent exploitation of vulnerabilities within its system that implicated the security of the PII and PHI of Plaintiff and the Washington Subclass;
- g. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to encrypt the sensitive PII and PHI of Plaintiff and the Washington Subclass, including their Social Security Numbers and/or confidential medical records;
- h. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to timely monitor and test its security measures in a manner sufficient to detect the unauthorized access and/or acquisition of the PII and PHI of Plaintiff and the Washington Subclass;
- i. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action after receiving inquiries regarding the possible sale of protected patient information on the Dark Web and thus failing to protect Plaintiff and the Washington Subclass's PII and PHI from further unauthorized disclosure, release, data breaches, and theft; and
- j. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff and the Washington Subclass's PII and PHI from further unauthorized disclosure, release, data breaches, and theft.

231. Defendant had statutory, regulatory, and common law obligations to prevent the foreseeable risk of harm to others, including the Plaintiff and the Washington Subclass.

232. It was foreseeable that the failure to use reasonable measures to protect the sensitive PII and PHI of Plaintiff and the Washington Subclass and to provide timely notice that a breach was detected if reasonable security measures were not taken, would put consumers, such as Plaintiff and the Washington Subclass at a serious risk of injury from the theft and fraudulent use of patients PII and PHI.

233. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and the Washington Subclass suffered injury and/or damages.

234. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

235. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PII and PHI of Plaintiff and the Washington Subclass and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Washington Subclass.

236. Plaintiff and the Washington Subclass seek relief under Wash. Rev. Code § 19.86.090, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

COUNT VII

VIOLATION OF THE WASHINGTON DATA BREACH STATUTE WASH. REV. CODE § 19.255.010(1), *ET. SEQ.* (ON BEHALF OF PLAINTIFF AND THE WASHINGTON SUBCLASS)

237. Plaintiff and the Washington Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 130.

238. Under § 19.255.010, Defendant is required to accurately notify Plaintiff and the Washington Subclass following discovery or notification of the breach of their data security system (if personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured) in the most expedient time possible and without unreasonable delay under Wash. Rev. Code Ann. § 19.255.010(1).

239. The Washington legislature, in passing § 19.255.010, recognized that data breaches of personal information, such as the Data Breach at issue here, can compromise financial security and be costly to consumers. The legislature intended to

strengthen the data breach notification requirements to better safeguard personal information, prevent identity theft, and [. . .] provide consumers whose personal information has been jeopardized due to a data breach with the information needed to secure financial accounts and make the necessary reports in a timely manner to minimize harm from identity theft.

Wash. Rev. Code Ann. § 19.255.010 [2015 c 64].

240. Defendant conducts business in Washington and owns or licenses computerized data that includes personal information as defined by Wash. Rev. Code Ann. § 19.255.010(1).

241. The PII and PHI of Plaintiff and the Washington Subclass (e.g., Social Security numbers) includes personal information as covered under Wash. Rev. Code Ann. § 19.255.010(5).

242. Because Defendant discovered a breach of its security system (in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured), Defendant had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code Ann. § 19.255.010(1) and § 19.255.010(8).

243. As a direct and proximate result of Defendant's violations of Wash. Rev. Code Ann. § 19.255.010(1), Plaintiff and the Washington Subclass suffered damages, as described above.

244. Plaintiff and the Washington Subclass seek relief under Wash. Rev. Code Ann. §§ 19.255.010(10)(a), 19.255.010(10)(b) including, but not limited to, actual damages and injunctive relief.

COUNT VIII

WASHINGTON UNIFORM HEALTH CARE INFORMATION ACT, WASH. REV. CODE §§ 70.02.020, *ET SEQ.*; § 70.02.170, *ET SEQ.* (ON BEHALF OF PLAINTIFF AND THE WASHINGTON SUBCLASS)

245. Plaintiff and the Washington Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 130.

246. Plaintiff brings this claim against Defendant, operating in Washington, on behalf of the Washington Subclass whose personal information and protected health information was compromised as a result of the Data Breach.

247. Defendant is a health care provider subject to Wash. Rev. Code § 70.02.020. As such, Defendant may not disclose health care information about a patient to any other person without the patient's written authorization.

248. As a result of conducting the business of providing health care in Washington, Defendant possessed personal information including personal health care information pertaining to Plaintiff and the Washington Subclass.

249. Defendant released personal information, including health care information, regarding Plaintiff and the Washington Subclass without authorization in violation of Wash. Rev. Code § 70.02.020.

250. Plaintiff and the Washington Subclass were injured and have suffered damages from Defendant's illegal disclosure and negligent release of their personal information, including health care information in violation of Wash. Rev. Code § 70.02.020 and § 70.02.150.

251. Plaintiff and the Washington Subclass seek relief under Wash. Rev. Code § 70.02.170, including, but not limited to, actual damages, nominal damages, injunctive relief, and/or attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the Washington Subclass, and appointing Plaintiff and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including, but not limited to, an order:

- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the PII and PHI of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including actual, consequential, nominal, and statutory damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

1 Date: January 14, 2022

Respectfully Submitted,

2 **HAGENS BERMAN SOBOL SHAPIRO LLP**

3 By: /s/ Thomas E. Loeser

4 THOMAS E. LOESER (WSB# 38701)

1301 Second Ave, Suite 2000

5 Seattle, WA 98101

6 Telephone: (206) 623-7292

7 Facsimile: (206) 623-0594

Email: toml@hbsslw.com

8 JOHN A. YANCHUNIS

9 *(Pro Hac Vice application to be filed)*

10 RYAN D. MAXEY

11 *(Pro Hac Vice application to be filed)*

12 **MORGAN & MORGAN COMPLEX**
13 **LITIGATION GROUP**

201 N. Franklin Street, 7th Floor

14 Tampa, FL 33602

15 Telephone: (813) 223-5505

16 Email: jyanchunis@ForThePeople.com

17 Email: rmaxey@ForThePeople.com

18 *Attorneys for Plaintiff and the Putative Class*

EXHIBIT 1

×Sea Mar offers COVID-19 first dose vaccines either by appointment or on a walk-in basis. For more information visit our [COVID-19 Vaccination Page](#).
For information and resources regarding COVID-19 visit our [COVID-19 page](#).

[About Us](#) [Services/Locations](#) [Patients/Clients](#) [Careers](#) [Give Now](#)

PATIENTS/CLIENTS

[Home](#)

Notice Privacy Practices

Protect Patient Information



This notice describes how medical information about you may be used. Please review it carefully.

Sea Mar Community Health Centers respects your privacy. We do not disclose your information to others unless you tell us to do so, or

The law protects the privacy of the health information we create and protect. Protected health information includes your symptoms, test results, diagnosis, billing and payment information relating to these services. Federal law allows us to use and disclose your information for purposes of treatment and health care operations to improve the quality of care and information for payment purposes.

Examples of Use and Disclosures of Protected Health Information for Treatment, Payment, and Health Operations.

For treatment:

Information obtained by a nurse, physician, or other member of our health care team will be recorded in your medical record. Your care information may be shared with other departments and disciplines within Sea Mar in order to facilitate coordination of your care. This is intended to help them stay informed about your care.

For payment:

When we request payment from your health insurance plan. Health plans need information from us about your medical care, your diagnoses, the procedures performed and/or the recommended care.

[About Us](#) [Services/Locations](#) [Patients/Clients](#) [Careers](#) [Give Now](#)

- ✓ We use your medical records to assess quality and improve services.
- ✓ We may use and disclose medical records to review the qualifications and performance of our health care providers and
- ✓ We may contact you to remind you about appointments and give you information about treatment alternatives or other
- ✓ We may contact you to raise funds.
- ✓ We may use and disclose your information to conduct or arrange for services, including:
 - medical quality review by your health plan;
 - accounting, legal, risk management, and insurance services;
 - audit functions, including fraud and abuse detection and compliance programs.

Your Health Information Rights

The health and billing records we create and store are the property of the practice/health care facility. The protected health

You have a right to:

- ✓ Receive, read, and ask questions about this Notice;
- ✓ Ask us to restrict certain uses and disclosures. You must deliver this request in writing to us. We are not required to gra
- ✓ Request and receive from us a paper copy of the most current Notice of Privacy Practices for Protected Health Informa
- ✓ Request that you be allowed to see and get a copy of your protected health information. You may make this request in v
- ✓ Have us review a denial of access to your health information—except in certain circumstances;
- ✓ Ask us to change your health information. You may give us this request in writing. You may write a statement of disagre
- and included with any release of your records.
- ✓ When you request, we will give you a list of disclosures of your health information. The list will not include disclosures t
- once every 12 months. We will notify you of the cost involved if you request this information more than once in 12 mon
- ✓ Ask that your health information be given to you by another means or at another location. Please sign, date, and give us
- ✓ Cancel prior authorizations to use or disclose health information by giving us a written revocation. Your revocation doe
- not affect any action taken before we have it. Sometimes, you cannot cancel an authorization if its purpose was to obtai

For help with these rights at this site, during normal business hours, please contact:

_____ [Responsible Person & Phone Number]
 _____ [Address]

Our Responsibilities. We are required to:

- ✓ Keep your protected health information private;

• Give us this Notice

- ✓ We have the right to change our practices regarding the protected health information we maintain. If we make changes You may receive the most recent copy of this Notice for it or by visiting our medical records department to pick one up.

To Ask for Help or Complain:

If you have questions, want more information, or want to report a problem about the handling of your protected health info your privacy rights have been violated, you may discuss your concerns with any staff member. You may also deliver a writte [Privacy Officer] at (206) 763-5210 or 1040 South Henderson, Seattle WA, 98108. You may also file a complaint with the U file a complaint with us or with the U.S. Secretary of Health and Human Services. If you complain, we will not retaliate again

Notification of Family and Others:

Unless you object, we may release health information about you to a friend or family member who is involved in your medic your care. We may tell your family or friends your condition and that you are in a hospital. In addition, we may disclose heal

We may use and disclose your protected health information without your authorization as follows:

- ✓ **With Medical Researchers**—if the research has been approved and has policies to protect the privacy of your health in preparing to conduct a research project.
- ✓ **To Funeral Directors/Coroners** consistent with applicable law to allow them to carry out their duties.
- ✓ **To Organ Procurement Organizations (tissue donation and transplant)** or persons who obtain, store, or transplant org
- ✓ **To the Food and Drug Administration (FDA)** relating to problems with food, supplements, and products.
- ✓ **To Comply With Workers' Compensation Laws**—if you make a workers' compensation claim.
- ✓ **For Public Health and Safety Purposes as Allowed or Required by Law:** to prevent or reduce a serious, immediate thre legal authorities; to protect public health and safety; to prevent or control disease, injury, or disability; to report vital st
- ✓ **To Report Suspected Abuse or Neglect** to public authorities.
- ✓ **To Correctional Institutions** if you are in jail or prison, as necessary for your health and the health and safety of others.
- ✓ **For Law Enforcement Purposes** such as when we receive a subpoena, court order, or other legal process, or you are the
- ✓ **For Health and Safety Oversight Activities.** For example, we may share health information with the Department of He
- ✓ **For Disaster Relief Purposes.** For example, we may share health information with disaster relief agencies to assist in nc
- ✓ **For Work-Related Conditions That Could Affect Employee Health.** For example, an employer may ask us to assess hea
- ✓ **To the Military Authorities of U.S. and Foreign Military Personnel.** For example, the law may require us to provide info
- ✓ **In the Course of Judicial/Administrative Proceedings** at your request, or as directed by a subpoena or court order.
- ✓ **For Specialized Government Functions.** For example, we may share information for national security purposes.

Uses and disclosures not in this Notice will be made only as allowed or required by law or with your written authorization.



Exceptional service. Every person. Every time.

Sea Mar Community Health Centers
Administrative Offices
1040 S. Henderson St.
Seattle, WA 98108

Copyright ©2020: Sea Mar Community Health Centers

EXHIBIT 2



Notice of Privacy Practices Acknowledgement

The Notice of Privacy Practices for Protected Health Information describes how medical information about you may be used and disclosed, how you can get access to this information and who to contact if you have questions, concerns or complaints.

Sea Mar has the responsibility to protect the privacy of your information, provide a Notice of Privacy Practices, and follow information practices that are described in this notice. If you have any questions, please contact Sea Mar's Vice President of Corporate and Legal Affairs at 206.763.5277.

By signing this form, you acknowledge receipt of Sea Mar Community Health Centers' Notice of Privacy Practices and Patient Rights and Responsibilities. Sea Mar encourages you to review these notices carefully.

I acknowledge receipt of Sea Mar Community Health Centers' Notice of Privacy Practices and Patient Rights and Responsibilities.

Patient or legally authorized individual signature

Date

Time

Printed name if signed on behalf of the patient

Relationship
(parent, legal guardian, personal representative)

Patient Name: <<PName>>

DOB: <<PDOB>>

Patient ID: <<PNumber>>

This form will be retained in your medical record.

EXHIBIT 3

Sea Mar Community Health Centers Notifies Patients of Data Security Incident

SEATTLE, WASHINGTON: October 29, 2021 – Sea Mar Community Health Centers (“Sea Mar”), a non-profit organization that provides healthcare services to underserved communities in the state of Washington, has learned of a data security incident that may have involved personal and protected health information belonging to certain current and former Sea Mar patients. Sea Mar has sent notification of this incident to potentially impacted individuals and has provided resources to assist them.

On June 24, 2021, Sea Mar was informed that certain Sea Mar data had been copied from its digital environment by an unauthorized actor. Upon receipt of this information, Sea Mar immediately took steps to secure its environment and commenced an investigation to determine what happened and to identify the specific information that may have been impacted. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result, Sea Mar learned that additional data may have been removed from its digital environment between December 2020 and March 2021. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals, which was completed on August 30, 2021.

Sea Mar is not aware of any evidence of the misuse of any information potentially involved in this incident. However, beginning on October 29, 2021, Sea Mar provided of this incident to the potentially impacted individuals. In so doing, Sea Mar provided information about the incident and about steps that potentially impacted individuals can take to protect their information. Sea Mar takes the security and privacy of patient information very seriously and is taking steps to prevent a similar event from occurring in the future.

The following personal and protected health information may have been involved in the incident: Name, address, Social Security number, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment.

Sea Mar has established a toll-free call center to answer questions about the incident and to address related concerns. Call center representatives are available Monday through Friday between 6:00 am – 3:30 pm Pacific Time and can be reached at 1-855-651-2684.

The privacy and protection of personal and protected health information is a top priority for Sea Mar, which deeply regrets any inconvenience or concern this incident may cause.

While we are not aware of the misuse of any potentially affected individual’s information, we are providing the following information to help those wanting to know more about steps they can take to protect themselves and their personal information:

What steps can I take to protect my personal information?

- Please notify your financial institution immediately if you detect any suspicious activity on any of your accounts, including unauthorized transactions or new accounts opened in our name that you do not recognize. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.
- You can request a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC’s website offers helpful information at www.ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your notification letter.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Use the following contact information for the three nationwide credit reporting agencies:

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors to possible fraudulent activity within your report and requests that your creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is included in the letter and is also listed at the bottom of this page.

How do I put a security freeze on my credit reports?

You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or online by following the instructions found at the websites listed below. You will need to provide the following information when requesting a security freeze (note that if you are making a request for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) address. You may also be asked to provide other personal information such as your email address, a copy of a government-issued identification card, and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. There is no charge to place, lift, or remove a freeze. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Experian Security Freeze
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion (FVAD)
PO Box 2000
Chester, PA 19022
1-800-909-8872
www.transunion.com

What should I do if my family member was involved in the incident and is deceased?

You may choose to notify the three major credit bureaus, Equifax, Experian and Trans Union, and request they flag the deceased credit file. This will prevent the credit file information from being used to open credit. To make this request, mail a copy of your family member's death certificate to each company at the addresses below.

Equifax
Equifax Information Services
P.O. Box 105169,
Atlanta, GA 30348

Experian
Experian Information Services
P.O. Box 9701
Allen, TX 75013

TransUnion
Trans Union Information
Services
P.O. Box 2000
Chester, PA 19022

EXHIBIT 4



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

November 5, 2021

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

We represent Sea Mar Community Health Centers ("Sea Mar"), a healthcare provider located in the state of Washington, in connection with a data security incident described in greater detail below. This letter is being sent because the personal information of certain Maine residents may have been affected by a recent data security incident experienced by Sea Mar. The incident may have involved unauthorized access to the Maine residents' names and Social Security numbers.

On June 24, 2021, Sea Mar was informed that certain Sea Mar data had been removed from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately took steps to secure its environment and commenced an investigation to determine what happened. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of this independent investigation, Sea Mar learned on August 12, 2021 that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

On October 22, 2021, Sea Mar learned of six (6) Maine residents within the potentially affected population whose personal information may have been affected as a result of the incident. An additional fifty-two (52) residents were notified pursuant to the Health Insurance Portability and Accountability Act of 1996.

Sea Mar notified the potentially affected Maine residents of this incident via the attached sample letter(s) beginning on October 29, 2021. In so doing, Sea Mar offered notified individuals whose Social Security numbers may have been involved complimentary identity protection services through

Attorney General Aaron Frey
November 5, 2021
Page 2

Kroll, a global leader in risk mitigation and response. Sea Mar has also reported this incident to the Federal Bureau of Investigation.

Please contact me should you have any questions.

Very truly yours,



Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl: Sample Consumer Notification Letter



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident, steps that you can take to help protect your information, and resources that Sea Mar is making available to assist you.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, Social Security number, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

To help relieve concerns and to help safeguard your identity following this incident, Sea Mar has secured the services of Kroll to provide identity monitoring services at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **January 27, 2022** to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

Additional information describing your services is included with this letter.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

Sea Mar also encourages you to take full advantage of the services offered to you through Kroll. Kroll representatives are available to answer questions or address concerns you may have. Kroll call center representatives are available Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holiday; and can be reached by calling 1-855-651-2684.

For More Information. If you have questions or need assistance, please call 1-855-651-2684, Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rogelio Riojas". The signature is fluid and cursive, with the first name "Rogelio" and last name "Riojas" clearly distinguishable.

Rogelio Riojas, Executive Director
Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident and steps that you can take to help protect your information.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

For More Information. Further information about how to help protect your personal information is included with this letter. If you have questions or need assistance, please contact 1-855-651-2684, Monday through Friday, 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Our representatives are fully versed on this incident and can answer any questions you may have.

Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rogelio Riojas". The signature is fluid and cursive, with the first name "Rogelio" and last name "Riojas" clearly distinguishable.

Rogelio Riojas, Executive Director
Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

EXHIBIT 5



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident, steps that you can take to help protect your information, and resources that Sea Mar is making available to assist you.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, Social Security number, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

To help relieve concerns and to help safeguard your identity following this incident, Sea Mar has secured the services of Kroll to provide identity monitoring services at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **January 27, 2022** to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

Additional information describing your services is included with this letter.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

Sea Mar also encourages you to take full advantage of the services offered to you through Kroll. Kroll representatives are available to answer questions or address concerns you may have. Kroll call center representatives are available Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holiday; and can be reached by calling 1-855-651-2684.

For More Information. If you have questions or need assistance, please call 1-855-651-2684, Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rogelio Riojas". The signature is fluid and cursive, with the first name "Rogelio" and last name "Riojas" clearly distinguishable.

Rogelio Riojas, Executive Director
Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident and steps that you can take to help protect your information.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

For More Information. Further information about how to help protect your personal information is included with this letter. If you have questions or need assistance, please contact 1-855-651-2684, Monday through Friday, 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Our representatives are fully versed on this incident and can answer any questions you may have.

Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rogelio Riojas". The signature is fluid and cursive, with the first name "Rogelio" and last name "Riojas" clearly distinguishable.

Rogelio Riojas, Executive Director
Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

EXHIBIT 6

23457



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident, steps that you can take to help protect your information, and resources that Sea Mar is making available to assist you.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, Social Security number, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

To help relieve concerns and to help safeguard your identity following this incident, Sea Mar has secured the services of Kroll to provide identity monitoring services at no cost to you for 24 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **January 27, 2022** to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>


Additional information describing your services is included with this letter.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

Sea Mar also encourages you to take full advantage of the services offered to you through Kroll. Kroll representatives are available to answer questions or address concerns you may have. Kroll call center representatives are available Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holiday; and can be reached by calling 1-855-651-2684.

For More Information. If you have questions or need assistance, please call 1-855-651-2684, Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rogelio Riojas". The signature is fluid and cursive, with the first name "Rogelio" and last name "Riojas" clearly distinguishable.

Rogelio Riojas, Executive Director
Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident and steps that you can take to help protect your information.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

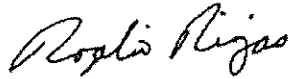
What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

For More Information. Further information about how to help protect your personal information is included with this letter. If you have questions or need assistance, please contact 1-855-651-2684, Monday through Friday, 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Our representatives are fully versed on this incident and can answer any questions you may have.

Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rogelio Riojas". The signature is fluid and cursive, with the first name "Rogelio" and last name "Riojas" clearly distinguishable.

Rogelio Riojas, Executive Director
Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

EXHIBIT 7



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident, steps that you can take to help protect your information, and resources that Sea Mar is making available to assist you.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, Social Security number, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

To help relieve concerns and to help safeguard your identity following this incident, Sea Mar has secured the services of Kroll to provide identity monitoring services at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **January 27, 2022** to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

Additional information describing your services is included with this letter.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

Sea Mar also encourages you to take full advantage of the services offered to you through Kroll. Kroll representatives are available to answer questions or address concerns you may have. Kroll call center representatives are available Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holiday; and can be reached by calling 1-855-651-2684.

For More Information. If you have questions or need assistance, please call 1-855-651-2684, Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rogelio Riojas". The signature is fluid and cursive, with the first name "Rogelio" and last name "Riojas" clearly distinguishable.

Rogelio Riojas, Executive Director
Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident and steps that you can take to help protect your information.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

For More Information. Further information about how to help protect your personal information is included with this letter. If you have questions or need assistance, please contact 1-855-651-2684, Monday through Friday, 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Our representatives are fully versed on this incident and can answer any questions you may have.

Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rogelio Riojas". The signature is fluid and cursive, with the first name "Rogelio" and last name "Riojas" clearly distinguishable.

Rogelio Riojas, Executive Director
Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

EXHIBIT 8



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

October 29, 2021

VIA ELECTRONIC MAIL

Attorney General Bob Ferguson
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
Email: SecurityBreach@atg.wa.gov

Re: Notice of Data Security Incident

Dear Attorney General Ferguson:

We represent Sea Mar Community Health Centers (“Sea Mar”), a healthcare provider located in the state of Washington, in connection with a data security incident described in greater detail below. This letter is being sent because the personal information of certain Washington residents may have been affected by a recent data security incident experienced by Sea Mar. The incident may have involved unauthorized access to the Washington residents’ names, Social Security numbers, dates of birth, medical information, and/or health insurance information.

On June 24, 2021, Sea Mar was informed that certain Sea Mar data had been removed from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately took steps to secure its environment and commenced an investigation to determine what happened. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of this independent investigation, Sea Mar learned on August 12, 2021 that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar notified 628,569 potentially affected Washington residents of this incident via the attached sample letter(s) beginning on October 29, 2021. In so doing, Sea Mar offered notified individuals whose Social Security numbers may have been involved complimentary identity protection services through Kroll, a global leader in risk mitigation and response. Sea Mar has also reported this incident to the Federal Bureau of Investigation.

Attorney General Bob Ferguson

October 29, 2021

Page 2

Please contact me should you have any questions.

Very truly yours,



Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl: Sample Consumer Notification Letter



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident, steps that you can take to help protect your information, and resources that Sea Mar is making available to assist you.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, Social Security number, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

To help relieve concerns and to help safeguard your identity following this incident, Sea Mar has secured the services of Kroll to provide identity monitoring services at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **January 27, 2022** to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

Additional information describing your services is included with this letter.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

Sea Mar also encourages you to take full advantage of the services offered to you through Kroll. Kroll representatives are available to answer questions or address concerns you may have. Kroll call center representatives are available Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holiday; and can be reached by calling 1-855-651-2684.

For More Information. If you have questions or need assistance, please call 1-855-651-2684, Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rogelio Riojas". The signature is fluid and cursive, with the first name "Rogelio" and last name "Riojas" clearly distinguishable.

Rogelio Riojas, Executive Director
Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident and steps that you can take to help protect your information.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

For More Information. Further information about how to help protect your personal information is included with this letter. If you have questions or need assistance, please contact 1-855-651-2684, Monday through Friday, 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Our representatives are fully versed on this incident and can answer any questions you may have.

Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rogelio Riojas". The signature is fluid and cursive, with the first name "Rogelio" and last name "Riojas" clearly distinguishable.

Rogelio Riojas, Executive Director
Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.